Amendments to the Claims

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently Amended) A method for secure key delivery for decrypting a distribution archive file containing a plurality of digital content documents at an ~~unsecure~~ unsecured site that receives a stream of distribution archive files from a publishing site, the method comprising:

(a) at the publishing site, encrypting each digital content document with a key to generate encrypted document content;

(b) at the publishing site, computing for each document a document identifier that is related to, but cannot be derived solely from, the encrypted content of that document;

(c) at the publishing site, creating a list of document identifier and decryption key pairs;

(d) at the publishing site, assembling the encrypted document content for each content document and the key pair list into a distribution archive file;

(e) at the publishing site, encrypting the distribution archive file with a scheduled key unique to that distribution archive file and placing the encrypted distribution file on the stream;

(f) at the unsecured site, selecting a distribution archive file from the stream;

(~~a~~g) at the unsecured site, extracting a scheduled key from ~~a first~~ the selected distribution archive file in the stream;

(~~b~~h) at the unsecured site, using the ~~retrieved~~ extracted scheduled key to decrypt the next subsequent distribution archive file in the stream following the ~~first~~ selected distribution archive file;

(i) removing the encrypted document content and the key pair list from the decrypted distribution archive file and storing them at the unsecured site; and

(~~c~~j) selecting the distribution archive file decrypted in step (h) and repeating steps (~~a~~g), (h), (i) and (~~b~~j) for each distribution archive file in the stream.

2. (Currently Amended) The method of claim 1 further comprising:

(~~d~~k) receiving a scheduled key ~~for~~ at the unsecured site to decrypt the first distribution archive file in the stream from the publishing site.

3. (Currently Amended) The method of claim 1 wherein ~~each distribution archive file comprises a plurality of encrypted content files and wherein the method further~~ step (e) comprises~~:~~

(~~d~~) encrypting, with a scheduled key, a distribution archive file including a scheduled key for the next distribution archive file in the stream and the plurality of encrypted content files.

4. (Currently Amended) The method of claim 1 wherein ~~each distribution archive file comprises a plurality of encrypted content files and wherein the method further~~ step (e) comprises~~:~~

(~~d~~) encrypting, with a scheduled key, a distribution archive file including the plurality of encrypted content files and a non-encrypted scheduled key for the next distribution archive file.

5. (Canceled).

6. (Currently Amended) The method of claim ~~5~~ 1 wherein step (~~g~~e) comprises generating a new scheduled key, encrypting the new scheduled key and including the encrypted scheduled key in the distribution archive file.

7. (Currently Amended) The method of claim ~~6~~ 1 wherein ~~the new scheduled key is encrypted~~ step (b) comprises for each document, computing the document identifier using a text string embedded in program code in the publishing site.

8. (Currently Amended) The method of claim ~~7~~ 1 wherein step (~~a~~g) comprises storing an extracted scheduled key in encrypted form.

9. (Currently Amended) The method of claim ~~8~~ 7 ~~wherein the extracted scheduled key is encrypted~~ further comprising recomputing a document identifier at the unsecured site with a text string embedded in program code located at the ~~unsecure~~ unsecured site.

10. (Currently Amended) The method of claim 9 wherein the text string embedded in program code in the publishing site is the same as the text string embedded in program code at the ~~unsecure~~ unsecured site.

11. (Currently Amended) ~~Apparatus~~An apparatus for secure key delivery for decrypting a distribution archive file containing a plurality of digital content documents at an ~~unsecure~~ unsecured site that receives a stream of distribution archive files from a publishing site, the apparatus comprising:

at the publishing site, an encryption engine that encrypts each digital content document with a key to generate encrypted document content;

at the publishing site, an OID calculator that computes for each document a document identifier that is related to, but cannot be derived solely from, the encrypted content of that document;

at the publishing site, means for creating a list of document identifier and decryption key pairs;

at the publishing site, means for assembling the encrypted document content for each content document and the key pair list into a distribution archive;

at the publishing site, means for encrypting the distribution archive file with a scheduled key unique to that distribution archive file;

at the unsecured site, a key decryptor that extracts a scheduled key from each distribution archive file in the stream;

means for temporarily storing the extracted scheduled key at the unsecured site; ~~and~~

at the unsecured site, a decryption engine that uses the stored scheduled key to decrypt the next distribution archive file in the stream following the distribution archive file from which the scheduled key was extracted; and

a file system that removes the encrypted document content and the key pair list from the decrypted archive file and stores them at the unsecured site.

12. (Original) The apparatus of claim 11 further comprising means for receiving a scheduled key for the first distribution archive file in the stream from the publishing site.

13. (Currently Amended) The apparatus of claim 11 wherein ~~each distribution archive file comprises a plurality of encrypted content files and wherein~~ the apparatus further comprises an encryption engine that encrypts, with a scheduled key, a distribution archive file including a scheduled key for the next distribution archive file in the stream and the plurality of encrypted content files.

14. (Currently Amended) The apparatus of claim 11 wherein ~~each distribution archive file comprises a plurality of encrypted content files and wherein~~ the apparatus further comprises an encryption engine that encrypts, with a scheduled key, a distribution archive file including the plurality of encrypted content files and a non-encrypted scheduled key for the next distribution archive file.

15. (Canceled).

16. (Currently Amended) The apparatus of claim ~~15~~ 11 wherein the means for encrypting the distribution archive with a scheduled key comprises a key generator that generates a new scheduled key, a key encryptor that encrypts the new scheduled key and means for including the encrypted scheduled key in the distribution archive.

17. (Currently Amended) The apparatus of claim ~~16~~ 11 wherein the ~~key encryptor~~ OID calculator encrypts the new scheduled key using a text string embedded in program code in the publishing site.

18. (Currently Amended) The apparatus of claim ~~17~~ 11 wherein the means for temporarily storing the extracted scheduled key comprises means for storing an extracted scheduled key in encrypted form.

19. (Currently Amended) The apparatus of claim ~~18 wherein the means for temporarily storing the extracted scheduled key comprises~~ 17 further comprising means for ~~encrypting the extracted scheduled key~~ recomputing a document identifier with a text string embedded in program code located at the ~~unsecure~~ unsecured site.

20. (Currently Amended) The apparatus of claim 19 wherein the text string embedded in program code in the publishing site is the same as the text string embedded in program code at the ~~unsecure~~ unsecured site.

21. (Currently Amended) A computer program product for secure key delivery for decrypting a distribution archive file containing a plurality of digital content files at an ~~unsecure~~ unsecured site that receives a stream of distribution archive files from a publishing site, the computer program product comprising a computer usable medium having computer readable program code thereon, including:

program code at the publishing site, for encrypting each digital content document with a key to generate encrypted document content;

program code at the publishing site, for computing for each document a document identifier that is related to, but cannot be derived solely from, the encrypted content of that document;

program code at the publishing site, for creating a list of document identifier and decryption key pairs;

program code at the publishing site, for assembling the encrypted document content for each content document and the key pair list into a distribution archive file; and

program code at the publishing site, for encrypting the distribution archive file with a scheduled key unique to that distribution archive file and for placing the encrypted distribution file on the stream;

program code at the unsecured site for extracting a scheduled key from each distribution archive file in the stream;

program code at the unsecured site for temporarily storing the extracted scheduled key; ~~and~~

program code at the unsecured site for using the stored scheduled key to decrypt the next distribution archive file in the stream following the distribution archive file from which the scheduled key was extracted; and

program code for removing the encrypted document content and the key pair list from the decrypted archive file and for storing them at the unsecured site.

22. (Original) The computer program product of claim 21 further comprising program code for receiving a scheduled key for the first distribution archive file in the stream from the publishing site.

23. (Currently Amended) The computer program product of claim 21 wherein ~~each distribution archive file comprises a plurality of encrypted content files and wherein~~ the computer program product further comprises:

program code for encrypting, with a scheduled key, a distribution archive file including a scheduled key for the next distribution archive file in the stream and the plurality of encrypted content files.

24. (Currently Amended) The computer program product of claim 21 wherein ~~each distribution archive file comprises a plurality of encrypted content files and wherein~~ the computer program product further comprises:

program code for encrypting, with a scheduled key, a distribution archive file including the plurality of encrypted content files and a non-encrypted scheduled key for the next distribution archive file.

25. (Canceled).

26. (Currently Amended) The computer program product of claim ~~25~~ 21 wherein the program code for encrypting the distribution archive file comprises program code for generating a new scheduled key, program code for encrypting the new scheduled key and program code for including the encrypted scheduled key in the distribution archive file.

27. (Currently Amended) The computer program product of claim ~~26~~ 21 wherein the program code for ~~encrypting the new scheduled key encrypts the new scheduled key~~ computing a document identifier computes the document identifier using a text string embedded in program code in the publishing site.

28. (Currently Amended) The computer program product of claim ~~27~~ 21 wherein the program code for temporarily storing the extracted scheduled key comprises program code for storing an extracted scheduled key in encrypted form.

29. (Currently Amended) The computer program product of claim 28 ~~wherein the~~ further comprising program code for ~~encrypting the extracted scheduled key~~

~~encrypts the extracted scheduled key~~ recomputing a document identifier with a text string embedded in program code located at the ~~unsecure~~ unsecured site.

30. (Currently Amended) The computer program product of claim 29 wherein the text string embedded in program code in the publishing site is the same as the text string embedded in program code at the ~~unsecure~~ unsecured site.